

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-308249

(43)Date of publication of application : 31.10.2003

(51)Int.Cl. G06F 12/14
G09C 1/00
H04L 9/14

(21)Application number : 2002-112109

(71)Applicant : SONY CORP

(22)Date of filing : 15.04.2002

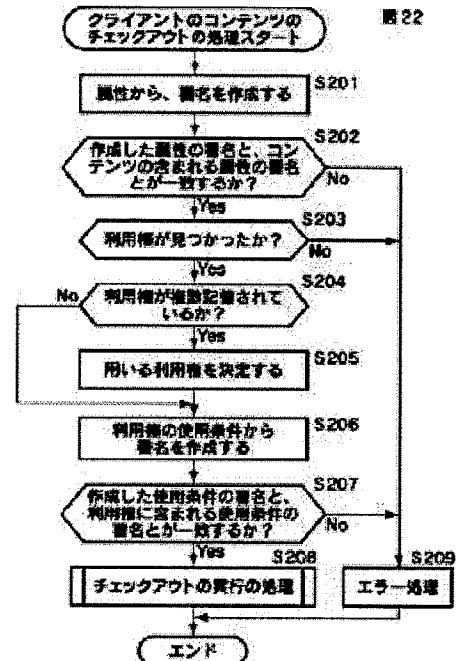
(72)Inventor : ISHIGURO RYUJI
TADA KEIKO
FUTAGAMI KISEI

(54) APPARATUS AND METHOD FOR INFORMATION PROCESSING, AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To securely prevent contents even in a contents storage device with low capability from illegally being used.

SOLUTION: A CPU selects contents stored in the contents storage device. In a step S202, the CPU verifies a 1st electronic signature added to the contents. A storage part stores a right to use. In a step S203, the CPU retrieves the right to use from the storage part. In a step S207, the CPU verifies a 2nd electronic signature added to the right to use. The CPU generates falsification detection data based upon information included in the right to use. In a step S208, the CPU outputs the use authorization, falsification detection data, and contents to the contents storage device on condition that neither the contents nor the right to use is falsified. This invention is applicable to a client of a DRM system.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-308249

(P2003-308249A)

(43)公開日 平成15年10月31日(2003.10.31)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 Z 5 B 0 1 7 3 1 0 K 5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1

審査請求 未請求 請求項の数 8 O L (全 24 頁)

(21)出願番号 特願2002-112109(P2002-112109)

(22)出願日 平成14年4月15日(2002.4.15)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 石黒 隆二

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 多田 恵子

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100082131

弁理士 稲本 義雄

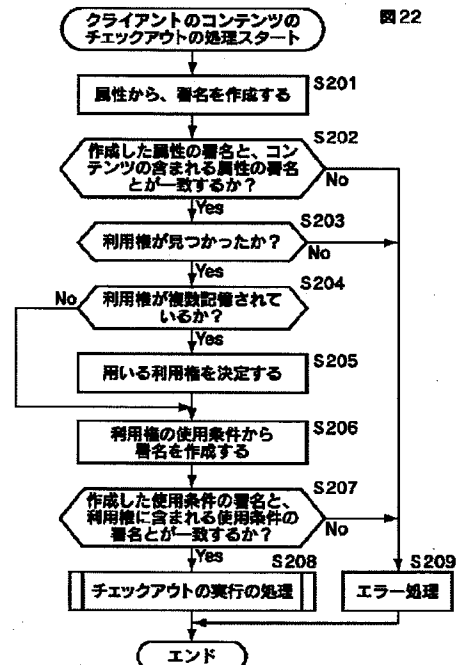
最終頁に続く

(54)【発明の名称】 情報処理装置および方法、並びにプログラム

(57)【要約】

【課題】 能力の低いコンテンツ記憶装置においても、コンテンツが不正に利用されるのを確実に防止する。

【解決手段】 CPUは、コンテンツ記憶装置に記憶させるコンテンツを選択する。ステップS202において、CPUは、コンテンツに付された第1の電子署名の検証を行う。記憶部は、利用権を記憶する。ステップS203において、CPUは、記憶部から利用権を検索する。ステップS207において、CPUは、利用権に付された第2の電子署名の検証を行う。CPUは、利用権に含まれている情報に基づき改竄検出データを生成する。ステップS208において、CPUは、コンテンツおよび利用権が改竄されていないとき、利用権と改竄検出データとコンテンツをコンテンツ記憶装置に出力する。本発明は、DRMシステムのクライアントに適用できる。



【特許請求の範囲】

【請求項1】 コンテンツに対応する利用権を基に前記コンテンツの利用を許可する情報処理装置において、コンテンツ記憶装置に記憶させる前記コンテンツを選択する第1の選択手段と、

前記第1の選択手段により選択された前記コンテンツに付された第1の電子署名の検証を行う第1の検証手段と、

前記第1の選択手段により選択された前記コンテンツの利用を許可する前記利用権を記憶する記憶手段と、

前記記憶手段から前記第1の選択手段により選択された前記コンテンツに対応する前記利用権を検索する検索手段と、

前記検索手段により検索された前記利用権に付された第2の電子署名の検証を行う第2の検証手段と、

前記検索手段により検索された前記利用権に含まれている情報に基づき第1の改竄検出データを生成する第1のデータ生成手段と、

前記第1の検証手段の検証結果、前記第2の検証手段の検証結果により前記コンテンツおよび前記利用権が改竄されていないと判定されたことを条件として、前記利用権と前記第1のデータ生成手段により生成された前記第1の改竄検出データと前記コンテンツを前記コンテンツ記憶装置に出力する第1の出力手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記検索手段により前記利用権が複数検索された場合、検索された複数の前記利用権から1つの前記利用権を選択する第2の選択手段を更に備え、前記第2の検証手段は前記第2の選択手段により選択された前記利用権に付された前記電子署名の検証を行い、前記第1のデータ生成手段は前記第2の選択手段により選択された前記利用権に含まれている情報に基づき前記第1の改竄検出データを生成することを特徴とする請求項1に記載の情報処理装置。

【請求項3】 前記第1の選択手段により選択された前記コンテンツを前記コンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に備え、

前記第1の出力手段は前記変換手段により変換された前記コンテンツを前記コンテンツ記憶装置に出力することを特徴とする請求項1に記載の情報処理装置。

【請求項4】 前記コンテンツに対応する前記利用権を前記コンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に備え、

前記第1のデータ生成手段により生成される前記第1の改竄検出データは前記変換手段により変換された前記利用権に基づく改竄検出データであることを特徴とする請求項1に記載の情報処理装置。

【請求項5】 前記第1のデータ生成手段が生成する前記第1の改竄検出データは前記利用権に含まれる使用条件に基づいて生成されることを特徴とする請求項1に記

載の情報処理装置。

【請求項6】 前記コンテンツ記憶装置から、前記コンテンツ記憶装置に記憶されている前記コンテンツに対応する前記利用権に基づいて前記第1のデータ生成手段により生成された前記第1の改竄検出データ全てを取得する取得手段と、

前記取得手段により取得された前記第1の改竄検出データ全体に基づいて第2の改竄検出データを生成する第2のデータ生成手段と、

10 前記第2のデータ生成手段により生成された前記第2の改竄検出データを前記コンテンツ記憶装置に出力する第2の出力手段とを更に備えることを特徴とする請求項1に記載の情報処理装置。

【請求項7】 コンテンツに対応する利用権を基に前記コンテンツの利用を許可する情報処理方法において、コンテンツ記憶装置に記憶させる前記コンテンツを選択する選択ステップと、

前記選択ステップの処理により選択された前記コンテンツに付された第1の電子署名の検証を行う第1の検証ステップと、

前記選択ステップの処理により選択された前記コンテンツの利用を許可する前記利用権の記憶手段への記憶を制御する記憶制御ステップと、

前記記憶手段から前記選択ステップの処理により選択された前記コンテンツに対応する前記利用権を検索する検索ステップと、

前記検索ステップの処理により検索された前記利用権に付された第2の電子署名の検証を行う第2の検証ステップと、

30 前記検索ステップの処理により検索された前記利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、

前記第1の検証ステップの処理の検証結果、前記第2の検証ステップの処理の検証結果により前記コンテンツおよび前記利用権が改竄されていないと判定されたことを条件として、前記利用権と前記データ生成ステップの処理により生成された前記改竄検出データと前記コンテンツを前記コンテンツ記憶装置に出力する出力ステップとを含むことを特徴とする情報処理方法。

40 【請求項8】 コンテンツに対応する利用権を基に前記コンテンツの利用を許可する情報処理を制御するコンピュータに、

コンテンツ記憶装置に記憶させる前記コンテンツを選択する選択ステップと、

前記選択ステップの処理により選択された前記コンテンツに付された第1の電子署名の検証を行う第1の検証ステップと、

前記選択ステップの処理により選択された前記コンテンツの利用を許可する前記利用権の記憶手段への記憶を制御する記憶制御ステップと、

前記記憶手段から前記選択ステップの処理により選択された前記コンテンツに対応する前記利用権を検索する検索ステップと、

前記検索ステップの処理により検索された前記利用権に付された第2の電子署名の検証を行う第2の検証ステップと、

前記検索ステップの処理により検索された前記利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、

前記第1の検証ステップの処理の検証結果、前記第2の検証ステップの処理の検証結果により前記コンテンツおよび前記利用権が改竄されていないと判定されたことを条件として、前記利用権と前記データ生成ステップの処理により生成された前記改竄検出データと前記コンテンツを前記コンテンツ記憶装置に出力する出力ステップとを実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラムに関し、特に、コンテンツとその利用権が別々に配布される著作権管理システムにおけるコンテンツを、著作権を保護しつつ、他の装置と受け渡しできるようにした、情報処理装置および方法、並びにプログラムに関する。

【0002】

【従来の技術】最近、インターネットを介して、音楽データや画像データ等のコンテンツをユーザーに配信するシステムが実現されている。

【0003】

【発明が解決しようとする課題】このような、著作物の著作権を保護するための従来のDRM (Digital Rights Management) システムにおいては、端末機的能力にかかわらず、同一の保護方式を用いているので、特に、能力の低い端末装置またはコンテンツ記憶装置において、コンテンツの不正な利用を防止することは困難であった。

【0004】また、利用権とコンテンツとを別々に配布するシステムにおいては、端末装置またはコンテンツ記憶装置において、両者の正当性を検証し、マッチングを行う処理は負荷が大きく、困難であった。例えば、コンテンツを処理能力の低い端末装置で、コンテンツに対応する利用権を保持していることを探し出し、その正当性を検証した上で、そのコンテンツの利用を許可するという実現するのは困難であった。

【0005】本発明はこのような状況に鑑みてなされたものであり、能力の低いコンテンツ記憶装置においても、コンテンツを利用できるようにすると共に、コンテンツが不正に利用されるのを確実に防止することができるようになるものである。

【0006】

【課題を解決するための手段】本発明の情報処理装置

は、コンテンツ記憶装置に記憶させるコンテンツを選択する第1の選択手段と、第1の選択手段により選択されたコンテンツに付された第1の電子署名の検証を行う第1の検証手段と、第1の選択手段により選択されたコンテンツの利用を許可する利用権を記憶する記憶手段と、記憶手段から第1の選択手段により選択されたコンテンツに対応する利用権を検索する検索手段と、検索手段により検索された利用権に付された第2の電子署名の検証を行う第2の検証手段と、検索手段により検索された利用権に含まれている情報に基づき第1の改竄検出データを生成する第1のデータ生成手段と、第1の検証手段の検証結果、第2の検証手段の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権と第1のデータ生成手段により生成された第1の改竄検出データとコンテンツをコンテンツ記憶装置に出力する第1の出力手段とを備えることを特徴とする。

【0007】情報処理装置は、検索手段により利用権が複数検索された場合、検索された複数の利用権から1つの利用権を選択する第2の選択手段を更に設け、第2の検証手段は第2の選択手段により選択された利用権に付された電子署名の検証を行い、第1のデータ生成手段は第2の選択手段により選択された利用権に含まれている情報に基づき第1の改竄検出データを生成するようにすることができる。

【0008】情報処理装置は、第1の選択手段により選択されたコンテンツをコンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に設け、第1の出力手段は変換手段により変換されたコンテンツをコンテンツ記憶装置に出力するようにすることができる。

【0009】情報処理装置は、コンテンツに対応する利用権をコンテンツ記憶装置に対応するフォーマットに変換する変換手段を更に設け、第1のデータ生成手段により生成される第1の改竄検出データは変換手段により変換された利用権に基づく改竄検出データとすることができる。

【0010】第1のデータ生成手段が生成する第1の改竄検出データは利用権に含まれる使用条件に基づいて生成されるようにすることができる。

【0011】情報処理装置は、コンテンツ記憶装置から、コンテンツ記憶装置に記憶されているコンテンツに対応する利用権に基づいて第1のデータ生成手段により生成された第1の改竄検出データ全てを取得する取得手段と、取得手段により取得された第1の改竄検出データ全体に基づいて第2の改竄検出データを生成する第2のデータ生成手段と、第2のデータ生成手段により生成された第2の改竄検出データをコンテンツ記憶装置に出力する第2の出力手段とを更に設けることができる。

【0012】本発明の情報処理方法は、コンテンツ記憶装置に記憶させるコンテンツを選択する選択ステップ

と、選択ステップの処理により選択されたコンテンツに付された第1の電子署名の検証を行う第1の検証ステップと、選択ステップの処理により選択されたコンテンツの利用を許可する利用権の記憶手段への記憶を制御する記憶制御ステップと、記憶手段から選択ステップの処理により選択されたコンテンツに対応する利用権を検索する検索ステップと、検索ステップの処理により検索された利用権に付された第2の電子署名の検証を行う第2の検証ステップと、検索ステップの処理により検索された利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、第1の検証ステップの処理の検証結果、第2の検証ステップの処理の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権とデータ生成ステップの処理により生成された改竄検出データとコンテンツをコンテンツ記憶装置に出力する出力ステップとを含むことを特徴とする。

【0013】本発明のプログラムは、コンピュータに、コンテンツ記憶装置に記憶させるコンテンツを選択する選択ステップと、選択ステップの処理により選択されたコンテンツに付された第1の電子署名の検証を行う第1の検証ステップと、選択ステップの処理により選択されたコンテンツの利用を許可する利用権の記憶手段への記憶を制御する記憶制御ステップと、記憶手段から選択ステップの処理により選択されたコンテンツに対応する利用権を検索する検索ステップと、検索ステップの処理により検索された利用権に付された第2の電子署名の検証を行う第2の検証ステップと、検索ステップの処理により検索された利用権に含まれている情報に基づき改竄検出データを生成するデータ生成ステップと、第1の検証ステップの処理の検証結果、第2の検証ステップの処理の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権とデータ生成ステップの処理により生成された改竄検出データとコンテンツをコンテンツ記憶装置に出力する出力ステップとを実行させることを特徴とする。

【0014】本発明の情報処理装置および方法、並びにプログラムにおいては、コンテンツ記憶装置に記憶させるコンテンツが選択され、選択されたコンテンツに付された第1の電子署名の検証が行われ、選択されたコンテンツの利用を許可する利用権が記憶される。そして、記憶手段から選択されたコンテンツに対応する利用権が検索され、検索された利用権に付された第2の電子署名の検証が行われる。検索された利用権に含まれている情報に基づき改竄検出データが生成される。さらに、第1の検証結果、第2の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権と改竄検出データとコンテンツがコンテンツ記憶装置に出力される。

【0015】コンテンツは、音声、画像、またはテキス

トなどの情報の方式にかかわらず有用な情報であれば良い。

【0016】電子署名は、生成の方式を問わず、正当性を保証するための情報であれば良い。

【0017】

【発明の実施の形態】図1は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット2には、クライアント1-1、1-2（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント1と称する）が接続されている。この例においては、クライアントが2台のみ示されているが、インターネット2には、任意の台数のクライアントが接続される。

【0018】また、インターネット2には、クライアント1に対してコンテンツを提供するコンテンツサーバ3、コンテンツサーバ3が提供するコンテンツを利用するのに必要な利用権をクライアント1に対して付与するライセンスサーバ4、およびクライアント1が利用権を受け取った場合に、そのクライアント1に対して課金処理を行う課金サーバ5が接続されている。

【0019】これらのコンテンツサーバ3、ライセンスサーバ4、および課金サーバ5も、任意の台数、インターネット2に接続される。

【0020】図2はクライアント1の構成を表している。

【0021】図2において、CPU（Central Processing Unit）21は、ROM（Read Only Memory）22に記憶されているプログラム、または記憶部28からRAM（Random Access Memory）23にロードされたプログラムに従って各種の処理を実行する。タイマ20は、計時動作を行い、時刻情報をCPU21に供給する。RAM23にはまた、CPU21が各種の処理を実行する上において必要なデータなども適宜記憶される。

【0022】暗号化復号部24は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部25は、例えば、ATRAC（Adaptive Transform Acoustic Coding）3方式などでコンテンツデータをエンコードし、入出力インタフェース32を介してドライブ30に接続されている半導体メモリ44に供給し、記録させる。あるいはまた、コーデック部25は、ドライブ30を介して半導体メモリ44より読み出した、エンコードされているデータをデコードする。

【0023】半導体メモリ44は、例えば、メモリースティック（商標）などにより構成される。

【0024】CPU21、ROM22、RAM23、暗号化復号部24、およびコーデック部25は、バス31を介して相互に接続されている。このバス31にはまた、入出力インタフェース32も接続されている。

【0025】入出力インタフェース32には、キーボー

ド、マウスなどよりなる入力部26、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部27、ハードディスクなどより構成される記憶部28、モデム、ターミナルアダプタなどより構成される通信部29が接続されている。通信部29は、インターネット2を介しての通信処理を行う。通信部29はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【0026】入出力インタフェース32にはまた、必要に応じてドライブ30が接続され、磁気ディスク41、光ディスク42、光磁気ディスク43、或いは半導体メモリ44などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部28にインストールされる。

【0027】なお、図示は省略するが、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5も、図2に示したクライアント1と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図2の構成は、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5などの構成としても引用される。

【0028】なお、図示は省略するが、PD (Portable Device) も、図2に示したクライアント1と基本的に同様の構成を有するコンピュータにより構成される。

【0029】次に、図3のフローチャートを参照して、クライアント1がコンテンツサーバ3からコンテンツの提供を受ける処理について説明する。

【0030】ユーザが、入力部26を操作することでコンテンツサーバ3に対するアクセスを指令すると、CPU21は、ステップS1において、通信部29を制御し、インターネット2を介してコンテンツサーバ3にアクセスさせる。ステップS2において、ユーザが、入力部26を操作して、提供を受けるコンテンツを指定すると、CPU21は、この指定情報を受け取り、通信部29から、インターネット2を介してコンテンツサーバ3に、指定されたコンテンツのコンテンツIDを通知する。図4のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ3は、暗号化されたコンテンツデータを含むコンテンツを送信してくるので、ステップS3において、CPU21は、通信部29を介して、このコンテンツデータを受信すると、ステップS4において、その暗号化されているコンテンツデータを記憶部28を構成するハードディスクに供給し、記憶させる。

【0031】次に、図4のフローチャートを参照して、クライアント1の以上の処理に対応するコンテンツサーバ3のコンテンツ提供処理について説明する。なお、以下の説明において、図2のクライアント1の構成は、コンテンツサーバ3の構成としても引用される。

【0032】ステップS21において、コンテンツサーバ3のCPU21は、インターネット2から通信部29を

介してクライアント1よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップS22に進み、クライアント1から送信されてきたコンテンツIDを取り込む。このコンテンツIDは、クライアント1が、図3のステップS2において通知してきた情報である。

【0033】ステップS23において、コンテンツサーバ3のCPU21は、記憶部28に記憶されているコンテンツの中から、ステップS22の処理で取り込まれたコンテンツIDで指定されたコンテンツデータを読み出す。CPU21は、ステップS24において、記憶部28から読み出されたコンテンツデータを、暗号化復号部24に供給し、コンテンツキーKcを用いて暗号化させる。

【0034】記憶部28に記憶されているコンテンツデータは、コーデック部25により、既にATRAC3方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【0035】なお、もちろん、記憶部28に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップS24の処理は省略することが可能である。

【0036】次に、ステップS25において、コンテンツサーバ3のCPU21は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキー情報(図5を参照して後述するEKBとK_{ENC}(Kc))を付加する。そして、ステップS26において、コンテンツサーバ3のCPU21は、ステップS24の処理で暗号化したコンテンツと、ステップS25の処理でキー情報を付加したヘッダとをフォーマット化したデータを、通信部29から、インターネット2を介して、アクセスしてきたクライアント1に送信する。

【0037】図5は、このようにして、コンテンツサーバ3からクライアント1にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ(Header)とデータ(Data)とにより構成される。

【0038】ヘッダには、コンテンツ情報(Content information)、URL(Uniform Resource Locator)、イネープリングキーブロック(有効化キーブロック)(EKB(Enabling Key Block))、EKBから生成されたキーK_{ENC}を用いて暗号化されたコンテンツキーKcとしてのデータK_{ENC}(Kc)、コンテンツの属性(Attributes)、および署名(Signatures)が配置されている。なお、EKBについては、図13および図14を参照して後述する。

【0039】コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するための識別情報としてのコンテンツID(CID)、そのコンテンツのコーデックの方式などの情報が含まれている。

【0040】URLは、そのコンテンツを利用するために

必要な利用権を取得するときアクセスするアドレス情報であり、図1のシステムの場合、具体的には、利用権を受けるために必要なライセンスサーバ4のアドレスである。

【0041】コンテンツの属性は、コンテンツに関する情報であり、コンテンツの属性には、コンテンツID、コンテンツの提供者を識別するための識別情報としてのレコードカンパニーID、アーティストを識別するための識別情報としてのアーティストIDなどが含まれる。本実施の形態では、属性は利用権の対象となるコンテンツを特定するために用いられる。

【0042】署名は、コンテンツの属性に対応する電子署名である。

【0043】データは、任意の数の暗号化ブロック (Encryption Block) により構成される。各暗号化ブロックは、イニシャルベクトル (IV (Initial Vector))、シード (Seed)、およびコンテンツデータをキーK'cで暗号化したデータE_{K'c}(data)により構成されている。

【0044】キーK'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適用して演算された値により構成される。K'c = Hash(Kc, Seed)

【0045】イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【0046】この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行われる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行われるCBC (Cipher Block Chaining) モードで行われる。

【0047】CBCモードの場合、最初の8バイトのコンテンツデータを暗号化するとき、その前段の8バイトの暗号化結果が存在しないため、最初の8バイトのコンテンツデータを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

【0048】このCBCモードによる暗号化を行うことで、1つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【0049】また、暗号方式についてはこれに限らない。

【0050】以上のようにして、クライアント1は、コンテンツサーバ3からコンテンツを無料で、自由に取得することができる。従って、コンテンツそのものは、大量に、配布することが可能となる。

【0051】しかしながら、各クライアント1は、取得したコンテンツを利用するとき、そのコンテンツの利用が許可されていることを示す利用権を保持している必要がある。そこで、図6を参照して、クライアント1がコンテンツを再生する場合の処理について説明する。

【0052】ステップS41において、クライアント1

のCPU21は、ユーザが入力部26を操作することで指示したコンテンツの識別情報 (CID) を取得する。この識別情報は、例えば、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【0053】そして、CPU21は、コンテンツが指示されると、そのコンテンツの属性 (Attributes) を読み取る。この属性 (Attributes) は、図5に示されるように、コンテンツのヘッダに記述されているものである。

【0054】次に、ステップS42に進み、CPU21は、ステップS41で読み取られた属性 (Attributes) が各利用権に含まれているコンテンツ条件を満たすような利用権が、クライアント1により既に取得され、記憶部28に記憶されているか否かを判定する。まだ、利用権が取得されていない場合には、ステップS43に進み、CPU21は、利用権取得処理を実行する。この利用権取得処理の詳細は、図7のフローチャートを参照して後述する。

【0055】ステップS42において、利用権が既に取得されていると判定された場合、または、ステップS43において、利用権取得処理が実行された結果、利用権が取得された場合、ステップS44に進み、CPU21は、取得されている利用権は有効期限内のものであるか否かを判定する。利用権が有効期限内のものであるか否かは、利用権の内容として規定されている期限 (後述する図8参照) と、タイマ20により計時されている現在日時と比較することで判断される。利用権の有効期限が既に満了していると判定された場合、CPU21は、ステップS45に進み、利用権更新処理を実行する。

【0056】ステップS44において、利用権はまだ有効期限内であると判定された場合、または、ステップS45において、利用権が更新された場合、ステップS46に進み、CPU21は記憶部28に記憶されている、利用権に含まれる使用条件及び使用状態 (後述する) を読み出し、再生の条件を満たしているかどうかを判定する。

【0057】ステップS46において、利用権に含まれる使用条件、及び使用状態に基づき、再生が許可されると判断された場合には、ステップS47に進み、CPU21は、暗号化されているコンテンツデータを記憶部28から読み出し、RAM23に格納させる。そして、ステップS48において、CPU21は、RAM23に記憶された暗号化コンテンツデータを、図5のデータに配置されている暗号化ブロック単位で、暗号化復号部24に供給し、コンテンツキーKcを用いて復号させる。

【0058】コンテンツキーKcを得る方法の具体例は、図13および図14を参照して後述するが、デバイスノードキー (DNK) を用いて、EKB (図5) に含まれるキーK_{EKB}を得ることができ、そのキーK_{EKB}を用いて、データK_{EKB} (Kc) (図5) から、コンテンツキーKcを得

ることができる。

【0059】CPU21は、さらに、ステップS49において、暗号化復号部24により復号されたコンテンツデータをコーデック部25に供給し、デコードさせる。そして、コーデック部25によりデコードされたデータを、CPU21は、入出力インタフェース32から出力部27に供給し、D/A変換させ、スピーカから出力させる。

【0060】ステップS46において、利用権に含まれる使用条件、及び使用状態に基づき、再生が許可されないと判断された場合、コンテンツを出力しないで、処理は終了する。

【0061】次に、図7のフローチャートを参照して、図6のステップS43で行われる利用権取得処理の詳細について説明する。

【0062】クライアント1は、事前にライセンスサーバに登録することにより、リーフID、DNK(Device Node Key)、クライアント1の秘密鍵・公開鍵のペア、ライセンスサーバの公開鍵、及び各公開鍵の証明書を含むサービスデータを取得しておく。

【0063】リーフIDは、クライアント毎に割り当てられた識別情報を表し、DNKは、コンテンツに含まれるEKB(有効化キープロック)によって暗号化されているコンテンツキーKcを復号するのに必要なデバイスノードキーである(図10を参照して後述する)。

【0064】最初にステップS61において、CPU21は、コンテンツのヘッダに記述されているURLを取得する。上述したように、このURLは、そのコンテンツを利用するために必要な利用権を取得するときアクセスすべきアドレスである。そこで、ステップS62において、CPU21は、ステップS61で取得したURLにアクセスする。具体的には、通信部29によりインターネット2を介してライセンスサーバ4にアクセスが行われる。このとき、ライセンスサーバ4は、クライアント1に対して、利用権のリストを送信するとともに、購入する利用権(コンテンツを使用するのに必要な利用権)を指定する利用権指定情報、並びにユーザIDとパスワードの入力を要求してくる(後述する図9のステップS102)。CPU21は、この要求を出力部27の表示部に表示させる。ユーザは、この表示に基づいて、入力部26を操作して、利用権指定情報、ユーザID、およびパスワードを入力する。なお、このユーザIDとパスワードは、クライアント1のユーザが、インターネット2を介してライセンスサーバ4にアクセスし、事前に取得しておいたものである。

【0065】CPU21は、ステップS63、S64において、入力部26から入力された利用権指定情報を取り込むとともに、ユーザIDとパスワードを取り込む。CPU21は、ステップS65において、通信部29を制御し、入力されたユーザIDとパスワードを、利用権指定情

報及びサービスデータ(後述する)に含まれるリーフIDを含む利用権要求をインターネット2を介してライセンスサーバ4に送信させる。

【0066】ライセンスサーバ4は、図9を参照して後述するように、ユーザIDとパスワード、並びに利用権指定情報に基づいて利用権を送信してくる(ステップS109)か、または、条件が満たされない場合には、利用権を送信してこない(ステップS112)。

【0067】ステップS66において、CPU21は、ライセンスサーバ4から利用権が送信されてきたか否かを判定し、利用権が送信されてきた場合には、ステップS67に進み、その利用権を記憶部28に供給し、記憶させる。

【0068】ステップS66において、利用権が送信されて来ないと判定した場合、CPU21は、ステップS68に進み、エラー処理を実行する。具体的には、CPU21は、コンテンツを利用するための利用権が得られないので、コンテンツの再生処理を禁止する。

【0069】以上のようにして、各クライアント1は、コンテンツを利用するために必要な利用権を取得して、初めて、そのコンテンツを使用することが可能となる。

【0070】なお、図7の利用権取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【0071】クライアント1に提供される利用権は、例えば、図8に示されるように、使用条件、リーフIDおよび電子署名などを含んでいる。

【0072】バージョンは、メジャーバージョンおよびマイナーバージョンをドットで区切って、利用権のバージョンを記述する情報である。

【0073】プロフィールは、10進の整数値から記述され、利用権の記述方法に対する制限を規定する情報である。

【0074】利用権IDは、16進数で記述される、利用権を識別するための識別情報である。

【0075】作成日時は、利用権が作成された日時を示す。

【0076】有効期限は、利用権の有効期限を示す。9999年23時59分59秒である有効期限は、有効期限に制限がないことを示す。

【0077】使用条件には、その利用権に基づいて、コンテンツを使用することが可能な使用期限、その利用権に基づいて、コンテンツを再生することが可能な再生期限、コンテンツの最大再生回数、その利用権に基づいて、コンテンツをコピーすることが可能な回数(許されるコピー回数)、最大チェックアウト回数、その利用権に基づいて、コンテンツをCD-Rに記録することができるか否か、PD(Portable Device)にコピーすることが可能な回数、利用権の移動の可否、使用ログをとる義務の有無等を示す情報が含まれる。

【0078】使用条件の電子署名は、使用条件に対応する、電子署名である。

【0079】定数は、使用条件または使用状態で参照される定数である。

【0080】リーフIDは、クライアントを識別するための識別情報である。

【0081】電子署名は、利用権全体に対応する、電子署名である。

【0082】証明書は、ライセンスサーバの公開鍵を含む証明書である。

【0083】また、クライアント1の記憶部28には、利用権の使用条件とあわせて、コンテンツや利用権の状態を表す情報である使用状態が記憶される。使用状態には、対応する利用権に基づいてコンテンツを再生した回数、コンテンツをコピーした回数、コンテンツをチェックアウトした回数、コンテンツを初めて再生した日時、コンテンツをCD-Rに記録した回数、その他コンテンツあるいは利用権に関する履歴情報等を示す情報が含まれる。

【0084】図6のステップS46の再生の条件の判定は、利用権に含まれる使用条件と、記憶部28に利用権と共に記憶されている使用状態とを基に行われる。例えば、使用状態に記憶されているコンテンツを再生した回数が、使用条件に含まれるコンテンツ最大再生回数より少ない場合には、再生の条件が満たされていると判定される。

【0085】次に、図9のフローチャートを参照して、図7のクライアント1の利用権取得処理に対応して実行されるライセンスサーバ4の利用権提供処理について説明する。なお、この場合においても、図2のクライアント1の構成は、ライセンスサーバ4の構成として引用される。

【0086】ステップS101において、ライセンスサーバ4のCPU21は、クライアント1よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップS102に進み、アクセスしてきたクライアント1に対して、各利用権に関する情報を含む利用権のリストを送信するとともに、ユーザIDとパスワード、並びに、利用権指定情報の送信を要求する。上述したようにして、クライアント1から、図7のステップS65の処理で、ユーザIDとパスワード、リーフID並びに利用権指定情報（利用権IDであってもよい）が送信されてきたとき、ライセンスサーバ4のCPU21は、通信部29を介してこれを受信し、取り込む処理を実行する。

【0087】そして、ライセンスサーバ4のCPU21は、ステップS103において、通信部29から課金サーバ5にアクセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ5は、インターネット2を介してライセンスサーバ4から与信処理の要求を受けると、そのユーザIDとパスワードに対応する

ユーザの過去の支払い履歴などを調査し、そのユーザが、過去に利用権の対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、利用権の付与を許容する与信結果を送信し、不払いの実績などがある場合には、利用権付与の不許可の与信結果を送信する。

【0088】ステップS104において、ライセンスサーバ4のCPU21は、課金サーバ5からの与信結果が、利用権を付与することを許容する与信結果であるか否かを判定し、利用権の付与が許容されている場合には、ステップS105に進み、ステップS102の処理で取り込まれた利用権指定情報に対応する利用権を、記憶部28に記憶されている利用権の中から取り出す。記憶部28に記憶されている利用権は、あらかじめ利用権ID、バージョン、作成日時、有効期限等の情報が記述されている。ステップS106において、CPU21は、その利用権に受信したリーフIDを付加する。さらに、ステップS107において、CPU21は、ステップS105で選択された利用権に対応づけられている使用条件を選択する。あるいはまた、ステップS102の処理で、ユーザから使用条件が指定された場合には、その使用条件が必要に応じて、予め用意されている使用条件に付加される。CPU21は、選択された使用条件を利用権に付加する。使用条件は利用権にあらかじめ付加されていてもよい。

【0089】ステップS108において、CPU21はライセンスサーバの秘密鍵により利用権に署名し、ライセンスサーバの公開鍵を含む証明書を利用権に添付し、これにより、図8に示されるような構成の利用権が生成される。

【0090】次に、ステップS109に進み、ライセンスサーバ4のCPU21は、その利用権（図8に示される構成を有する）を、通信部29からインターネット2を介してクライアント1に送信させる。

【0091】ステップS110においてライセンスサーバ4のCPU21は、ステップS109の処理で、いま送信した利用権（使用条件、リーフIDを含む）を、ステップS102の処理で取り込まれたユーザIDとパスワードに対応して、記憶部28に記憶させる。さらに、ステップS111において、CPU21は、課金処理を実行する。具体的には、CPU21は、通信部29から課金サーバ5に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、利用権の付与を要求したとしても、利用権を受けることができないことになる。

【0092】すなわち、この場合には、課金サーバ5から利用権の付与を不許可とする与信結果が送信されてく

10

20

30

40

50

るので、ステップS104からステップS112に進み、CPU21は、エラー処理を実行する。具体的には、ライセンスサーバ4のCPU21は、通信部29を制御してアクセスしてきたクライアント1に対して、利用権を付与することができない旨のメッセージを送信し、処理を終了させる。

【0093】この場合、上述したように、そのクライアント1は利用権を受けることができないので、そのコンテンツを利用すること（暗号化されたコンテンツデータを復号し、再生すること）ができないことになる。

【0094】本発明においては、図10に示されるように、ブロードキャストインクリプション（Broadcast Encryption）方式の原理に基づいて、デバイスとキーが管理される。キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイス固有のキーに対応する。本発明のシステムに用いられる階層ツリー構造鍵管理については特許公開2001-352321号公報に記載されている。図10の例の場合、番号0から番号15までの16個のデバイスに対応するキーが生成される。

【0095】各キーは、図中丸印で示されるツリー構造の各ノードに対応して規定される。この例では、最上段のルートノードに対応してルートキーKRが、2段目のノードに対応してキーK0、K1が、3段目のノードに対応してキーK00乃至K11が、第4段目のノードに対応してキーK000乃至キーK111が、それぞれ対応されている。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーK0000乃至K1111が、それぞれ対応されている。

【0096】階層構造とされているため、例えば、キーK0010とキー0011の上位のキーは、K001とされ、キーK000とキーK001の上位のキーは、K00とされている。以下同様に、キーK00とキーK01の上位のキーは、K0とされ、キーK0とキーK1の上位のキーは、KRとされている。

【0097】コンテンツを利用するキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの1つのパスの各ノードに対応するキーで管理される。例えば、番号3のリーフに対応するデバイスにおいて、コンテンツを利用するためのキーは、キーK0011、K001、K00、K0、KRを含むパスの各キーで

管理される。【0098】本発明のシステムにおいては、図11に示されるように、図10の原理に基づいて構成されるキーシステムで、デバイスのキーとコンテンツのキーの管理が行われる。図11の例では、8+24+32段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そし

て、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

【0099】すなわち、このTシステムのノードよりさらに下の階層の24段のノードに対応するキーにより、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスが対応される。この例の場合、これにより、2²⁴（約16メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の32段の階層により、2³²（約4ギガ）のユーザ（あるいはクライアント1）を規定することができる。最下段の32段のノードからTシステムのノードまでのパス上の各ノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【0100】コンテンツを暗号化したコンテンツキーは更新されたルートキーKR'によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、EKB（図13および図14を参照して後述する）内に配置される。EKBにおける末端から1つ上の段の更新ノードキーはEKBの末端のノードキーあるいはリーフキーによって暗号化され、EKB内に配置される。クライアント1は、サービスデータに記述されているDNKのいずれかのキーを用いて、コンテンツデータとともに配布されるEKB（図13および図14）内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、EKB内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、クライアント1は、更新ルートキーKR'を得ることができる。

【0101】図12に階層ツリー構造のカテゴリの分類の具体的な例を示す。図12において、階層ツリー構造の最上段には、ルートキーKR2301が設定され、以下の中間段にはノードキー2302が設定され、最下段には、リーフキー2303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーからなるデバイスノードキー（DNK）を保有する。

【0102】最上段から第M段目（図11の例では、M=8）の所定のノードがカテゴリノード2304として設定される。すなわち第M段目のノードの各々が特定カテゴリのデバイス設定ノードとされる。第M段の1つのノードを頂点としてM+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとされる。

【0103】例えば図12の第M段目の1つのノード2305にはカテゴリ「メモリスティック（商標）」が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴ

10

20

30

40

50

リ専用のノードまたはリーフとして設定される。すなわち、ノード2305以下が、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義される。

【0104】さらに、M段から数段分下位の段をサブカテゴリノード2306として設定することができる。図12の例では、カテゴリ「メモリスティック」ノード2305の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器]のノード2306が設定され、さらに、サブカテゴリノードである再生専用器のノード2306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード2307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる「PHS」ノード2308と、「携帯電話」ノード2309が設定されている。

【0105】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZに、その頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0106】このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【0107】また、ある時点tにおいて、デバイス3の所有する鍵K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキーK001, K00, K0, KRを、それぞれ

新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）tの更新キーであることを示す。

【0108】更新キーの配布処理について説明する。キーの更新は、例えば、図13に示す有効化キーブロック（EKB: Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルを、ネットワークを介して、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。なお、有効化キーブロック（EKB）は、図10に示されるようなツリー構造を構成する各リーフ（最下段のノード）に対応するデバイスに、新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（EKB）は、キー更新ブロック（KRB: Key Renewal Block）と呼ばれることもある。

【0109】図13に示す有効化キーブロック（EKB）は、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図13の例は、図10に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図10から明らかなように、デバイス0、デバイス1は、更新ノードキーとしてK(t)00, K(t)0, K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001, K(t)00, K(t)0, K(t)Rが必要である。

【0110】図13のEKBに示されるように、EKBには複数の暗号化キーが含まれる。図13の最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーK0010によってこの暗号化キーを復号し、更新ノードキーK(t)001を得ることができる。また、復号により得た更新ノードキーK(t)001を用いて、図13の下から2段目の暗号化キーEnc(K(t)001, K(t)00)が復号可能となり、更新ノードキーK(t)00を得ることができる。

【0111】以下順次、図13の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号することで、更新ノードキーK(t)0が得られ、これを用いて、図13の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号することで、更新ルートキーK(t)Rが得られる。

【0112】一方、ノードキーK000は更新する対象に含まれておらず、ノード0, 1が、更新ノードキーとして必要なのは、K(t)00, K(t)0, K(t)Rである。ノード0, 1は、デバイスキーK0000,

K0001を用いて、図13の上から3段目の暗号化キーEnc(K000, K(t)00)を復号することで更新ノードキーK(t)00を取得し、以下順次、図13の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号することで、更新ノードキーK(t)0を得、図13の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号することで、更新ルートキーK(t)Rを得る。このようにして、デバイス0, 1, 2は更新したキーK(t)Rを得ることができる。

【0113】なお、図13のインデックスは、図の右側の暗号化キーを復号するための復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0114】図10に示すツリー構造の上位段のノードキーK(t)0, K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図14の有効化キープロック(EKB)を用いることで、更新ノードキーK(t)00をデバイス0, 1, 2に配布することができる。

【0115】図14に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図10に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のコンテンツキーK(t)conが必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新コンテンツキーK(t)conを暗号化したデータEnc(K(t)00, K(t)con)が、図14に示されるEKBとともに配布される。この配布により、デバイス4など、その他のグループの機器が復号することができないデータとしての配布が可能となる。

【0116】すなわち、デバイス0, 1, 2はEKBを処理して得たキーK(t)00を用いて暗号文を復号すれば、t時点でのコンテンツキーK(t)conを得ることが可能になる。

【0117】図15に、t時点でのコンテンツキーK(t)conを得る処理例として、K(t)00を用いて新たな共通のコンテンツキーK(t)conを暗号化したデータEnc(K(t)00, K(t)con)と、図14に示すEKBとを記録媒体を介して受領したデバイス0の処理を示す。すなわちこの例は、EKBによる暗号化メッセージデータをコンテンツキーK(t)conとした例である。

【0118】図15に示すように、デバイス0は、記録媒体に格納されている世代t時点のEKBと、自分があるかじめ格納しているノードキーK000を用いて、上述したと同様のEKB処理により、ノードキーK(t)00を生成する。さらに、デバイス0は、復号した更新ノードキーK(t)00を用いて、更新コンテンツキー

K(t)conを復号して、後にそれを使用するために自分だけが持つリーフキーK0000で暗号化して格納する。

【0119】図16に有効化キープロック(EKB)のフォーマット例を示す。バージョン601は、有効化キープロック(EKB)のバージョンを示す識別子である。なお、バージョンは、最新のEKBを識別する機能と、コンテンツとの対応関係を示す機能を持つ。デブスは、有効化キープロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ603は、有効化キープロック(EKB)中のデータ部606の位置を示すポインタであり、タグポインタ604はタグ部607の位置、署名ポインタ605は署名608の位置を示すポインタである。

【0120】データ部606は、例えば更新するノードキーを暗号化したデータを格納する。例えば図15に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0121】タグ部607は、データ部606に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図18を用いて説明する。

【0122】図17では、データとして先に図13で説明した有効化キープロック(EKB)を送付する例を示している。この時のデータは、図17のBで示す表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この例の場合は、ルートキーの更新キーK(t)Rが含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータEnc(K(t)0, K(t)R)は、図17のAで示す階層ツリーに示す位置P0に対応する。次の段のデータは、Enc(K(t)00, K(t)0)であり、ツリー上では前のデータの左下の位置P00に対応する。ツリー構造の所定の位置から見て、その下に、データがある場合は、タグが0、ない場合はタグが1に設定される。タグは{左(L)タグ, 右(R)タグ}として設定される。表Bの最上段のデータEnc(K(t)0, K(t)R)に対応する位置P0の左下の位置P00にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図17のCで示すデータ列、およびタグ列が構成される。

【0123】タグは、対応するデータEnc(Kxxx, Kyyy)が、ツリー構造のどこに位置しているのかを示すために設定されるものである。データ部606に格納されるキーデータEnc(Kxxxx, Kyyy)・・・は、単純に暗号化されたキーの羅列データに過ぎないが、上述したタグによってデータとして格納された暗号化キーのツリー上の位置が判別可能となる。上述したタグを用いずに、先の図15で説明した構成のよう

に、暗号化データに対応させたノード・インデックスを用いて、例えば、

0: Enc (K (t) 0, K (t) R)

00: Enc (K (t) 00, K (t) 0)

000: Enc (K (t) 000, K (t) 00)

・・・のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると、冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0124】図16に戻って、EKBフォーマットについてさらに説明する。署名 (Signature) 608は、有効化キープブロック (EKB) を発行した例えば鍵管理センタ (ライセンスサーバ4)、コンテンツロバイダ (コンテンツサーバ3)、決済機関 (課金サーバ5) 等が実行する電子署名である。EKBを受領したデバイスは、署名検証によって正当な有効化キープブロック (EKB) 発行者が発行した有効化キープブロック (EKB) であることを確認する。

【0125】以上のようにして、ライセンスサーバ4から供給された利用権に基づいて、コンテンツサーバ3から供給されたコンテンツを利用する処理をまとめると、図18に示されるようになる。

【0126】すなわち、コンテンツサーバ3からクライアント1に対してコンテンツが提供されるとともに、ライセンスサーバ4からクライアント1にライセンスが与えられる。クライアント1をライセンスサーバ4に登録した際に供給されるサービスデータと、特定のコンテンツの利用を許可する情報である利用権との組み合わせをライセンスと呼ぶ。コンテンツは、コンテンツキーKcにより、暗号化されており (Enc (Kc, Content))、コンテンツキーKcは、更新ルートキーKR' (EKBから得られるキーであって、図5におけるキーK_{EKB}に対応する) で暗号化され (Enc (KR', Kc))、EKBとともに、暗号化されたコンテンツに付加されてクライアント1に提供される。

【0127】図18の例におけるEKBには、例えば、図19に示されるように、DNKで復号可能な更新ルートキーKR'が含まれている (Enc (DNK, KR'))。従って、クライアント1は、サービスデータに含まれるDNKを利用して、EKBから更新ルートキーKR'を得ることができる。さらに、更新ルートキーKR'を用いて、Enc (KR', Kc) からコンテンツキーKcを復号することができ、コンテンツキーKcを用いて、Enc (Kc, Content) からコンテンツを復号することができる。

【0128】このように、クライアント1にDNKを各デバイスに割り当てることにより、図10と図15を参照して説明した原理に従って、個々のクライアント1のリボーク (revoke) が可能になる。

【0129】また、ライセンスリーフIDを付加して配布することにより、クライアント1において、サービスデータと利用権の対応付けが行われることになり、利用権の不正コピーを防止することが可能になる。

【0130】また、クライアント用の証明書と秘密鍵をサービスデータとして配信するようにすることで、エンドユーザも、これらを用いて不正コピーを防止可能なコンテンツを作成することが可能になる。

【0131】本発明においては、図11を参照して説明したように、カテゴリノードにライセンスを管理するTシステムと、各種のコンテンツを利用するデバイスのカテゴリが対応づけられるので、複数のDNKを同一のデバイスに持たせることができる。その結果、異なるカテゴリのコンテンツを1つのデバイスで管理することが可能となる。

【0132】図20は、この関係の一例を表している。すなわち、デバイスD1には、Tシステムに基づいて、DNK1が割り当てられており、EKBを含むコンテンツ1を再生することができる。同様に、このデバイスD1には、例えば、DNK2が割り当てられており、メモリースティックにCDからリッピングしたコンテンツ2を記録することができる。この場合、デバイスD1は、コンテンツ1とコンテンツ2という、異なるシステム (Tシステムとデバイス管理システム) により配信されたコンテンツを同時に扱うことが可能となる。新たなDNKを割り当てるとき、既に割り当てられているDNKを削除するなどして、デバイスに1個のDNKだけを対応させるようにした場合、このようなことはできない。

【0133】このように、本発明においては、カテゴリ毎に独立したキー管理が可能になる。

【0134】また、DNKを、機器やメディアに予め埋め込むのではなく、ライセンスサーバ4により、登録処理を行う際に、各機器やメディアにダウンロードするようにすることで、ユーザによるキーの購入が可能なシステムを実現することができる。

【0135】コンテンツとその利用権を別々に配布するシステムにおいては、コンテンツは、それが作成された後、どのような使われ方をされようとも、その使われ方に関わりなく、全ての用途において、使用可能であるのが望ましい。例えば、異なるコンテンツ配信サービス、あるいは用途が異なる場合においても、同一のコンテンツが使えることが望ましい。本発明においては、このため、上述したように、各ユーザ (クライアント1) に、認証局としてのライセンスサーバ4から秘密鍵と、それに対応する公開鍵の証明書 (certificates) が配布される。各ユーザは、その秘密鍵を用いて、署名 (signature) を作成し、コンテンツに付加して、コンテンツの真正さ (integrity) を保証し、かつコンテンツの改竄防止を図ることができる。

【0136】次に、クライアント1から、クライアント

10

20

30

40

50

1に装着された、セキュアなメディアであり、コンテンツ記憶装置の一例であるメモリスティック（商標）へのコンテンツのチェックアウトの処理を説明する。

【0137】図21は、メモリスティックの構成を示す図である。メモリスティック651は、フラッシュメモリ（不揮発性メモリ）661、メモリコントロールブロック662、およびDES（Data Encryption Standard）の暗号化回路を含むセキュリティブロック663が1チップ上にIC化されたものである。

【0138】フラッシュメモリ661は、メモリコントロールブロック662の制御の基に、符号化され、暗号化されたコンテンツを記憶する。

【0139】メモリコントロールブロック662は、シリアル/パラレル変換、またはパラレル/シリアル変換を実行すると共に、供給されたコマンドおよびデータとを分離して、分離されたコマンドを実行する。メモリコントロールブロック662は、供給されたコマンドに対応して、コンテンツをフラッシュメモリ661に記憶させるか、またはフラッシュメモリ661に記憶されているコンテンツを読み出す。

【0140】メモリスティック651のセキュリティブロック663は、複数の認証キーとメモリカード毎にユニークなストレージキーを記憶する。セキュリティブロック663は、乱数発生回路を有し、メモリコントロールブロック662の制御の基に、クライアント1と相互認証し、セッションキーを共有する。

【0141】セキュリティブロック663は、後述する使用条件およびMAC値を含むインデックスを記憶する。

【0142】セキュリティブロック663は、メモリコントロールブロック662の制御の基に、暗号化されているコンテンツを復号する。

【0143】図22は、クライアント1によるコンテンツのチェックアウトの処理を説明するフローチャートである。

【0144】ステップS201において、クライアント1のCPU21は、チェックアウトするコンテンツを選択して、選択したコンテンツに含まれる属性から署名を作成する。

【0145】例えば、クライアント1のCPU21は、コンテンツに含まれる属性を、証明書に含まれるライセンスサーバの公開鍵で暗号化処理することにより、署名を作成する。

【0146】ステップS202において、クライアント1のCPU21は、作成した属性の署名と、コンテンツに含まれる属性の署名とを比較し、作成した属性の署名と、コンテンツに含まれる属性の署名とが一致したと判定された場合、属性は改竄されていないので、ステップS203に進む。

【0147】ステップS202において、作成した属性

の署名と、コンテンツに含まれる属性の署名とが一致しないと判定された場合、属性が改竄されているので、ステップS209に進み、クライアント1のCPU21は、エラー表示などのエラー処理を実行し、チェックアウトの実行の処理を行わないで、処理は終了する。

【0148】ステップS203において、クライアント1のCPU21は、対象となるコンテンツの属性が利用権に含まれるコンテンツ条件を満たし、チェックアウトが許可されている利用権を記憶部28から検索する。対象のコンテンツを利用するための利用権が記憶部28に見つからない場合には、ステップS209に進み、クライアント1のCPU21はエラー表示などの、エラー処理を実行し、チェックアウトの実行の処理を行わないで、処理は終了する。

【0149】ステップS203において、コンテンツを利用するための利用権が見つかった場合には、S204に進み、クライアント1のCPU21はコンテンツを利用するための利用権が記憶部28に1つ記憶されているか、複数記憶されているかを判定する。

【0150】記憶部28に対象のコンテンツを利用するための利用権が複数記憶されていると判定された場合、ステップS205に進み、クライアント1のCPU21は、出力部27のディスプレイに各利用権の使用条件等の情報を表示させ、どの利用権の使用条件をチェックアウトされたコンテンツの使用条件として用いるかをユーザに確認させ、ユーザからの入力部26への入力を基に、いずれの利用権をチェックアウトに用いるかを決定する。

【0151】ステップS205における利用権の選択は、ユーザによる選択に限らず、所定の規則に基づき優先順位が決定されるようになっていても構わない。

【0152】記憶部28に対象のコンテンツを利用するための利用権が1つ記憶されていると判定された場合、チェックアウトに用いられる利用権は決まっているので、ステップS205の利用権の選択は行われず、ステップS206に進む。

【0153】コンテンツを利用するための利用権の選択が行われた後、S206において、クライアント1のCPU21は、利用権の使用条件から署名を作成する。

【0154】例えば、クライアント1のCPU21は、利用権に含まれる使用条件を、証明書に含まれるライセンスサーバの公開鍵で暗号化処理することにより、署名を作成する。

【0155】ステップS207において、クライアント1のCPU21は、作成した使用条件の署名と、利用権に含まれる使用条件の署名とを比較し、作成した使用条件の署名と、利用権に含まれる使用条件の署名とが一致したと判定された場合、使用条件は改竄されていないので、ステップS208に進む。ステップS208において、クライアント1のCPU21は、チェックアウトの実

行の処理を行い、処理は終了する。

【0156】ステップS207において、作成した属性の署名と、コンテンツに含まれる属性の署名とが一致しないと判定された場合、属性が改竄されているので、ステップS209に進み、クライアント1のCPU21は、エラー表示などのエラー処理を実行し、チェックアウトの実行の処理を行わないで、処理は終了する。

【0157】図23は、ステップS208の処理に対応する、クライアント1のチェックアウトの実行の処理を説明するフローチャートである。

【0158】ステップS221において、クライアント1のCPU21は、装着されているメモリスティックと相互認証の処理を実行する。例えば、クライアント1のCPU21とメモリスティック651のセキュリティブロック663は、チャレンジアンドレスポンス方式の相互認証の処理を実行することができる。

【0159】ステップS221の処理において、相互認証されなかった場合、クライアント1またはメモリスティック651が、正当ではないので、ステップS222乃至S228の処理はスキップされ、コンテンツをメモリスティック651に書き込まないで、処理は終了する。

【0160】ステップS221の処理において、相互認証された場合、クライアント1およびメモリスティック651が、正当なので、クライアント1およびメモリスティック651は、共通の一時鍵（セッションキー）を共有し、ステップS222乃至S228の処理が実行される。

【0161】共通の一時鍵（セッションキー）が共有された以下の処理において、クライアント1がメモリスティック651に送信する情報は、暗号化復号部24において、一時鍵で暗号化される。また、クライアント1がメモリスティック651から受信した情報は、一時鍵により暗号化されているので、暗号化復号部24により、復号される。

【0162】ステップS222において、クライアント1のCPU21は、コンテンツをメモリスティック651に書き込む。例えば、クライアント1のCPU21は、メモリスティック651から、メモリスティック651のコンテンツキーを取得し、メモリスティック651のコンテンツキーに、コンテンツの鍵をかけ直して（コンテンツをメモリスティック651のコンテンツキーで暗号化して）、メモリスティック651のコンテンツキーに、鍵をかけ直したコンテンツをメモリスティック651に供給する。

【0163】なお、メモリスティック651に、コンテンツの鍵をかけ直させるようにしてもよい。

【0164】ステップS223において、クライアント1のCPU21は、利用権の使用条件のフォーマットをメモリスティックに対応する方式に変換する。

【0165】ステップS224において、クライアント1のCPU21は、暗号化復号部24に、利用権の使用条件のメッセージ認証符号（MAC：Message authenticationCode）（以下、MAC値とも称する）を算出させる。

【0166】DES暗号処理構成を用いたMAC値生成例を図24に示す。図24の構成に示すように対象となるメッセージ（使用条件）を8バイト単位に分割し、（以下、分割されたメッセージをM1、M2、・・・、MNとする）、まず、初期値（IV）とM1を、演算部24-1Aにより排他的論理和する（その結果をI1とする）。次に、I1をDES暗号化部24-1Bに入れ、鍵（以下、K1とする）を用いて暗号化する（出力をE1とする）。続けて、E1およびM2を演算部24-2Aにより排他的論理和し、その出力I2をDES暗号化部24-2Bへ入れ、鍵K1を用いて暗号化する（出力E2）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。DES暗号化部24-NBから最後に出てきたENがメッセージ認証符号（MAC（Message Authentication Code））となる。

【0167】ステップS225において、クライアント1のCPU21は、ステップS223の処理でフォーマットが変換された使用条件を、ステップS224の処理で算出されたMAC値と共にメモリスティック651のインデックスに書き込む。

【0168】図25は、メモリスティック651に記憶されているインデックスおよびコンテンツを説明する図である。

【0169】メモリスティック651のインデックス701には、コンテンツに対応して、コンテンツの使用条件、MAC値、およびポインタが格納される。インデックス701のポインタは、コンテンツのアドレスを格納している。

【0170】例えば、メモリスティック651に記憶されているコンテンツ702-1を示すポインタは、コンテンツ702-1の使用条件およびそのMAC値と共に、インデックス701に格納される。メモリスティック651に記憶されているコンテンツ702-2を示すポインタは、コンテンツ702-2の使用条件およびそのMAC値と共に、インデックス701に格納される。メモリスティック651に記憶されているコンテンツ702-3を示すポインタは、コンテンツ702-3の使用条件およびそのMAC値と共に、インデックス701に格納される。

【0171】ステップS226において、クライアント1のCPU21は、メモリスティック651から、ステップS225の処理により、新たに使用条件およびMAC値が書き込まれたインデックス701を取得する。

【0172】ステップS227において、クライアント1のCPU21は、新たに使用条件およびMAC値が書き

10

20

30

40

50

込まれたインデックス701を基に、メモリスティック651全体のインテグリティ・チェック値(ICV)を算出する。

【0173】インデックス701のインテグリティ・チェック値は、例えばインデックス701に対するハッシュ関数を用いて計算され、 $ICV = hash(Kicv, R1, R2, \dots)$ によって計算される。KicvはICV生成キーである。L1、L2は使用条件の情報であり、使用条件のMAC値が使用される。

【0174】ステップS228において、クライアント1のCPU21は、メモリスティック651のインテグリティ・チェック値を、算出したインテグリティ・チェック値に書き換えて、処理は終了する。

【0175】例えば、クライアント1のCPU21は、メモリスティック651から取得したインデックス701に含まれる、コンテンツ702-1乃至702-3に対応するMAC値を基に、インテグリティ・チェック値を算出する。

【0176】クライアント1のCPU21は、図25に示すように、メモリスティック651に、算出したインテグリティ・チェック値703を書き込む。

【0177】クライアント1は、インテグリティ・チェック値を一時鍵で暗号化して、メモリスティック651に送信する、いわゆる、SAC(Secure Authentication Channel)を介して、インテグリティ・チェック値をメモリスティック651に送信する。

【0178】このようにすることで、メモリスティックには、インデックス701に対応した、インテグリティ・チェック値703が安全に格納されることになる。

【0179】例えばコンテンツ再生時にインデックス701を基に生成したICVと、使用条件に基づいて生成したICV703とを比較して同一のICVが得られれば使用条件に改竄のないことが保証され、ICVが異なれば、改竄があったと判定される。

【0180】図26のフローチャートを参照して、図23に示すクライアント1のチェックアウトの実行の処理に対応する、メモリスティック651のチェックアウトの実行の処理を説明する。

【0181】ステップS241において、メモリスティック651のセキュリティブロック663は、クライアント1のステップS221の処理に対応して、クライアント1との相互認証の処理を実行する。

【0182】相互認証された場合、クライアント1およびメモリスティック651において、共通の一時鍵(セッションキー)が共有される。

【0183】共通の一時鍵(セッションキー)が共有された以下の処理において、メモリスティック651がクライアント1に送信する情報は、セキュリティブロック663において、一時鍵により暗号化される。また、メモリスティック651がクライアント1から受信し

た情報は、一時鍵により暗号化されているので、メモリスティック651のセキュリティブロック663は、暗号化されている情報を、一時鍵で復号する。

【0184】ステップS242において、メモリスティック651のメモリコントロールブロック662は、ステップS222の処理を実行するクライアント1からコンテンツが送信されてくるので、このコンテンツを受信して、コンテンツをフラッシュメモリ661に記憶させる。

【0185】ステップS243において、メモリスティック651のメモリコントロールブロック662は、ステップS225の処理を実行するクライアント1からフォーマットが変換された使用条件が送信されてくるので、使用条件を受信し、受信した使用条件をセキュリティブロック663のインデックス701に書き込む。また、メモリスティック651は、使用条件に対応させて、ステップS242の処理で記憶したコンテンツを示すポインタをセキュリティブロック663のインデックス701に書き込む。

【0186】ステップS243の処理により、図25に示すように、新たに記憶されたコンテンツに対応する使用条件、MAC値、およびコンテンツを示すポインタが、セキュリティブロック663のインデックス701に格納されることになる。

【0187】ステップS244において、メモリスティック651のメモリコントロールブロック662は、クライアント1から要求があるので、インデックス701をセキュリティブロック663から読み出し、読み出したインデックス701をクライアントに送信する。ステップS244の処理で送信されたインデックス701を受信することにより、クライアント1は、ステップS226の処理において、インデックス701を取得できる。

【0188】ステップS245において、メモリスティック651は、ステップS228の処理を実行するクライアント1から、新たなICVが送信されてくるので、クライアント1から送信されたICVを受信して、受信したICVを基に、ICVを更新し、処理は終了する。

【0189】このように、integrity情報である公開鍵暗号による署名がコンテンツに付され、共通鍵暗号方式によるハッシュ値によるintegrity情報が、クライアントにより生成され、データ記憶媒体の使用条件に付される。コンテンツのintegrity情報と使用条件のintegrity情報とが合わせて1つの情報として、インデックス701として管理されることになる。

【0190】このように、クライアント1は、メモリスティックの処理能力が低くとも、メモリスティックにおいて、コンテンツの保護のレベルを低下させることなく、公開鍵暗号方式による署名が付いたコンテンツ

を、メモリースティックにチェックアウトすることができるようになる。

【0191】処理能力が低い端末機においても、同一のコンテンツを使用することができるようになる。これにより、特に、あらゆるデバイス同士が、コンテンツをやりとりできるようになる。

【0192】すなわち、コンテンツをメモリースティックに書き込むようにした場合には、メモリースティックにコンテンツを記憶させることができる。

【0193】電子署名が付されているコンテンツのコンテンツ記憶装置への書き込みを制御し、コンテンツを利用するために必要な利用権の使用条件をコンテンツ記憶装置に対応するフォーマットに変換し、フォーマットが変換された使用条件の改竄を検出するための使用条件改竄検出データを生成し、フォーマットが変換された使用条件および使用条件改竄検出データのコンテンツ記憶装置への書き込みを制御するようにした場合には、能力の低いメモリースティックにおいても、コンテンツを利用できるようになると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【0194】コンテンツを記憶するメモリを設けるようにした場合には、コンテンツを記憶することができる。

【0195】また、情報処理装置から提供された、電子署名が付されているコンテンツの記憶を制御し、情報処理装置から供給された、使用条件、および使用条件の改竄を検出するための使用条件改竄検出データの記憶を制御するようにした場合には、能力が低い場合であっても、コンテンツを利用できるようになると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【0196】コンテンツ記憶装置であるメモリースティックに記憶させるコンテンツを選択し、選択されたコンテンツに付された第1の電子署名の検証を行い、選択されたコンテンツの利用を許可する利用権を記憶し、記憶部28から選択されたコンテンツに対応する利用権を検索し、検索された利用権に付された第2の電子署名の検証を行い、検索された利用権に含まれている情報に基づき改竄検出データを生成し、第1の検証結果、第2の検証結果によりコンテンツおよび利用権が改竄されていないと判定されたことを条件として、利用権と改竄検出データとコンテンツをコンテンツ記憶装置に出力する場合には、能力の低いメモリースティックにおいても、コンテンツを利用できるようになると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【0197】クライアントからメモリースティックにコンテンツをチェックアウトする例を説明したが、クライアントからメモリースティックにコンテンツをコピーするようにしても良く、コンテンツを移動するようにしても良い。

【0198】また、クライアントからメモリースティックにコンテンツをチェックアウトする例を説明したが、クライアントからコンテンツ記憶装置の他の例であるPDにコンテンツをチェックアウト、移動、またはコピーするようにしてもよい。

【0199】さらに、クライアントからPDに装着されているメモリースティックにコンテンツをチェックアウト、移動、またはコピーするようにしてもよい。この場合において、相互認証の処理は、クライアントおよびPDの間で実行され、PDおよびメモリースティックの間で実行される。

【0200】本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA(Personal Digital Assistants)、携帯電話機、ゲーム端末機などとすることができる。

【0201】一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0202】この記録媒体は、図2に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク41(フレキシブルディスクを含む)、光ディスク42(CD-ROM(Compact Disk-Read Only Memory)、DVD(Digital Versatile Disk)を含む)、光磁気ディスク43(MD(Mini-Disk)(商標)を含む)、もしくは半導体メモリ44などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM22や、記憶部28に含まれるハードディスクなどで構成される。

【0203】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0204】また、セキュリティに関連する処理を実行させるプログラムは、その処理を解析されるのを防ぐため、そのプログラム自体が暗号化されているのが望ましい。例えば、暗号処理などを行う処理については、そのプログラムをタンパーレジスタントモジュールとして構成することができる。

【0205】また、上記実施例では、コンテンツを利用するために必要な利用権を特定するためにコンテンツの属性と利用権のコンテンツ条件を用いたが、これに限らない。例えば、コンテンツに、該コンテンツを利用するために必要な利用権の利用権IDを含むようにしても良

く、この場合、コンテンツを指定すればそれを利用するために必要な利用権は一意に決まるため、両者のマッチングを決定する処理を行う必要はない。

【0206】

【発明の効果】以上のように、本発明によれば、コンテンツ記憶装置にコンテンツを記憶させることができる。

【0207】また、本発明によれば、能力の低いコンテンツ記憶装置においても、コンテンツを利用できるようにすると共に、コンテンツが不正に利用されるのを確実に防止することができる。

【図面の簡単な説明】

【図1】本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図2】図1のクライアントの構成を示すブロック図である。

【図3】図1のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図4】図1のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

【図5】図4のステップS26におけるフォーマットの例を示す図である。

【図6】図1のクライアントのコンテンツ再生処理を説明するフローチャートである。

【図7】図6のステップS43の利用権取得処理の詳細を説明するフローチャートである。

【図8】利用権の構成を示す図である。

【図9】図1のライセンスサーバの利用権提供の処理を説明するフローチャートである。

【図10】キーの構成を説明する図である。

【図11】カテゴリノードを説明する図である。

【図12】ノードとデバイスの対応の具体例を示す図である。

【図13】有効化キープブロックの構成を説明する図である。

【図14】有効化キープブロックの構成を説明する図であ*

＊る。

【図15】有効化キープブロックの利用を説明する図である。

【図16】有効化キープブロックのフォーマットの例を示す図である。

【図17】有効化キープブロックのタグの構成を説明する図である。

【図18】DNKを用いたコンテンツの復号処理を説明する図である。

10 【図19】有効化キープブロックの例を示す図である。

【図20】複数のコンテンツの1つのデバイスに対する割り当てを説明する図である。

【図21】メモリスティックの構成を示す図である。

【図22】コンテンツのチェックアウトの処理を説明するフローチャートである。

【図23】クライアントのチェックアウトの実行の処理を説明するフローチャートである。

【図24】DES暗号処理構成を用いたMAC値生成例を示す図である。

20 【図25】メモリスティックに記憶されているインデックスおよびコンテンツを説明する図である。

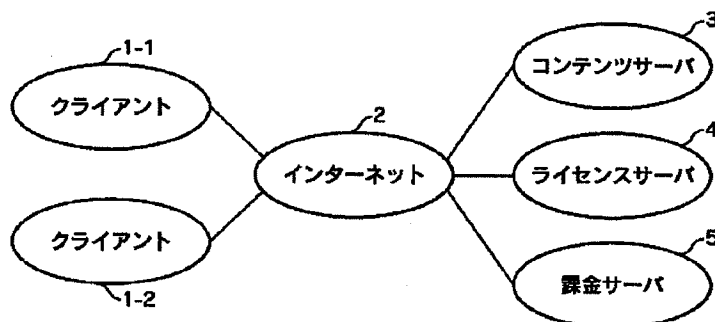
【図26】メモリスティックのチェックアウトの実行の処理を説明するフローチャートである。

【符号の説明】

1-1, 1-2 クライアント, 2 インターネット, 3 コンテンツサーバ, 4 ライセンスサーバ, 5 課金サーバ, 20 タイマ, 21 CPU, 24 暗号化復号部, 25 コーデック部, 26 入力部, 27 出力部, 28 記憶部, 29 通信部, 30 651 メモリスティック, 661 フラッシュメモリ, 662 メモリコントロールブロック, 663 セキュリティブロック, 701 インデックス, 702-1乃至702-3 コンテンツ, 703 ICV

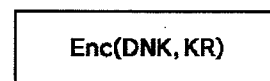
【図1】

図1

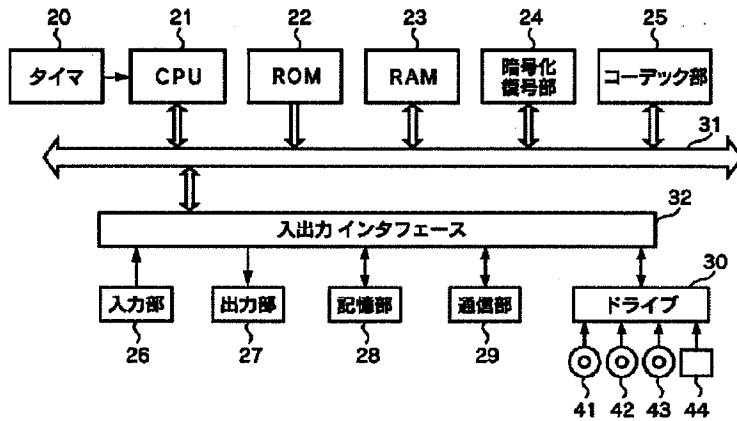


【図19】

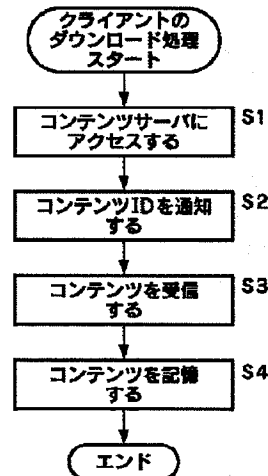
図19
EKB



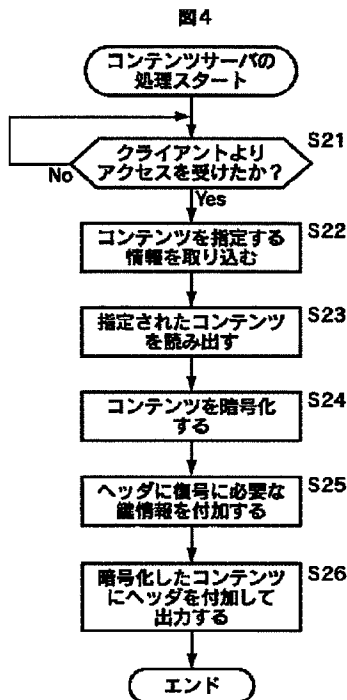
【図2】



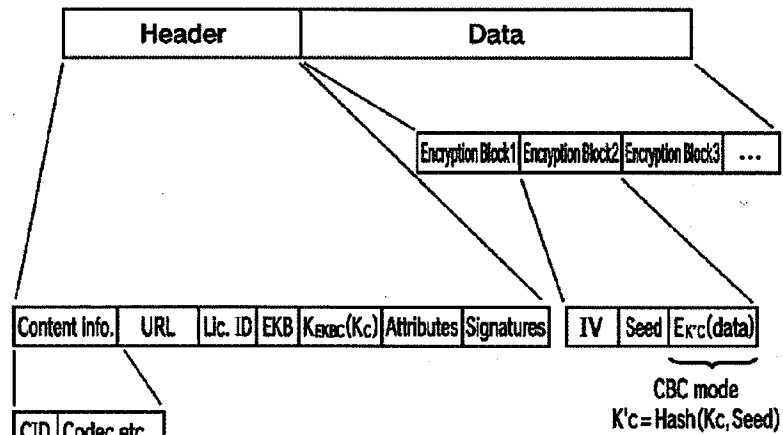
【図3】



【図4】



【図5】

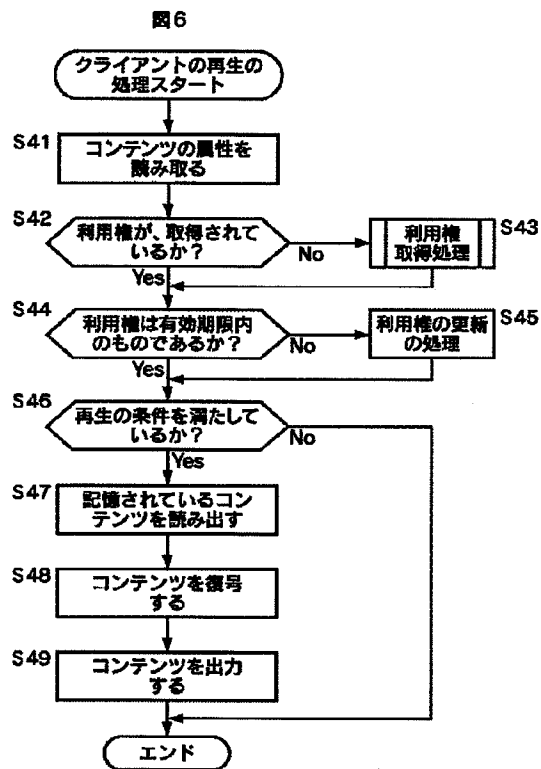


【図13】

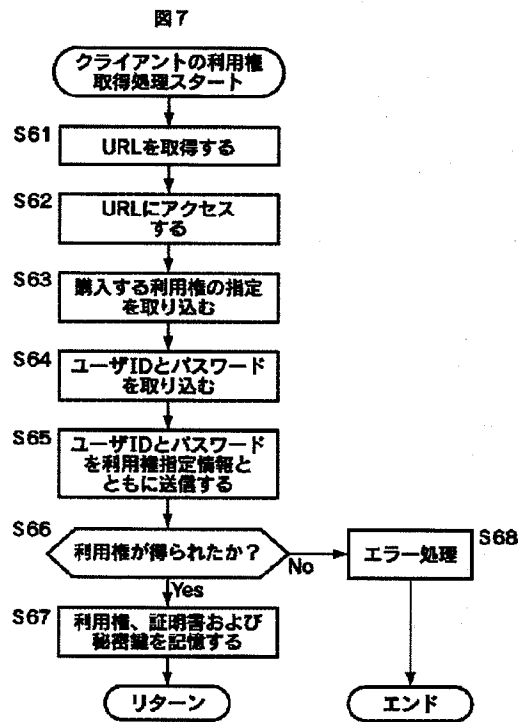
図13

バージョン (Version) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

【図6】



【図7】



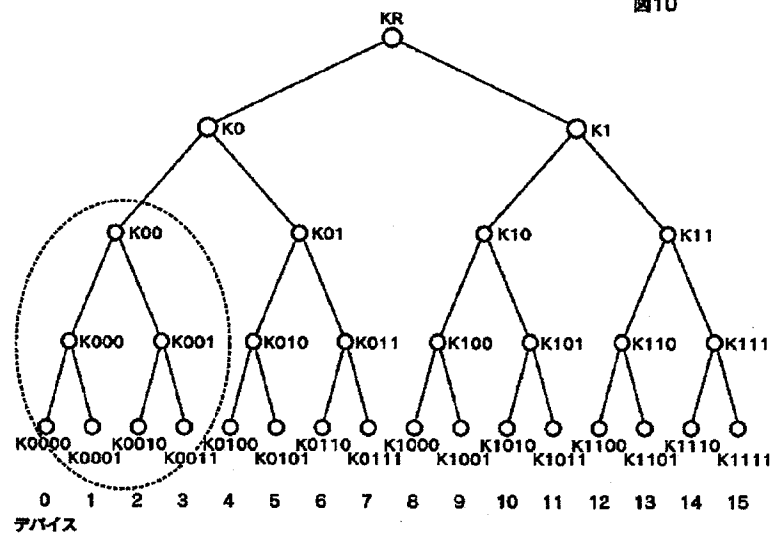
【図8】

図8

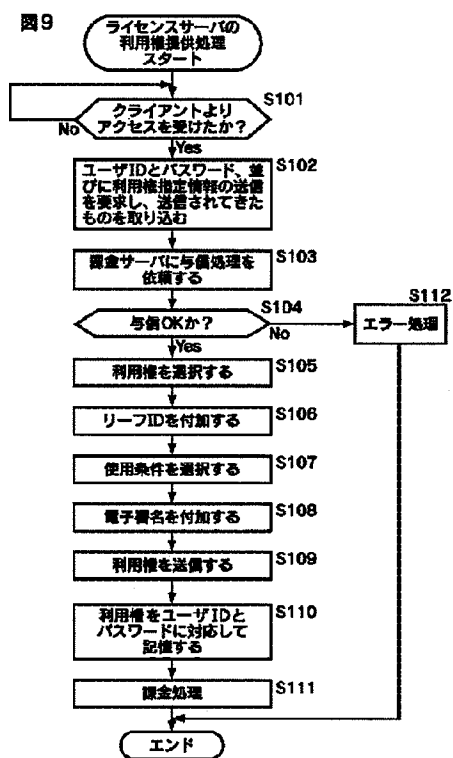
バージョン
プロファイル
利用権ID
作成日時
有効期限
使用条件
使用条件の電子署名
コンテンツ条件
定数
リーフID
電子署名
証明書

【図10】

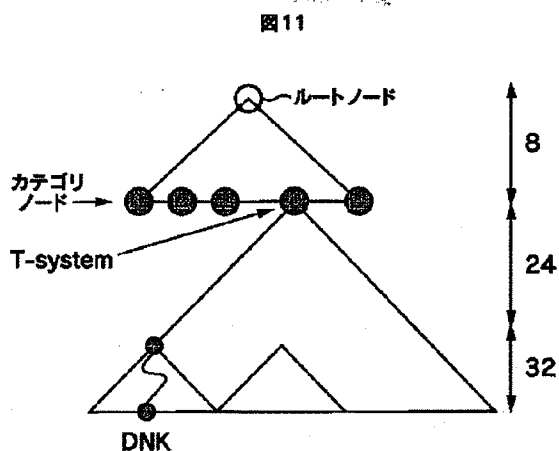
図10



【図9】



【図11】



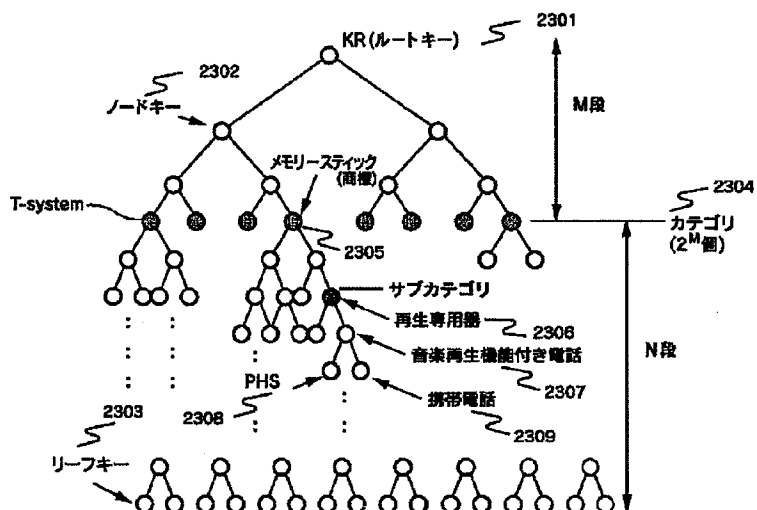
【図14】

図14

バージョン(Version) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

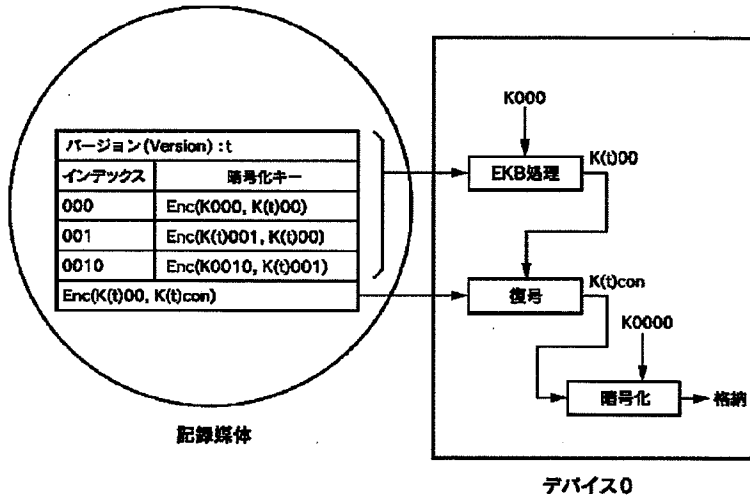
【図12】

図12



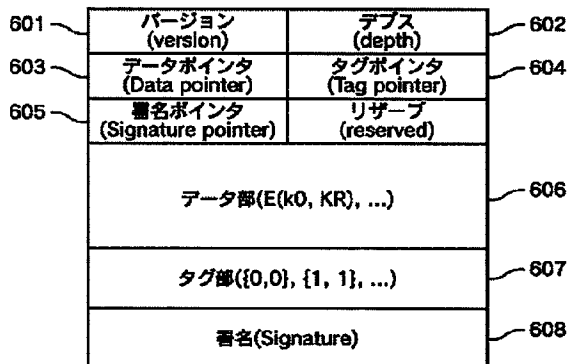
【図15】

図15



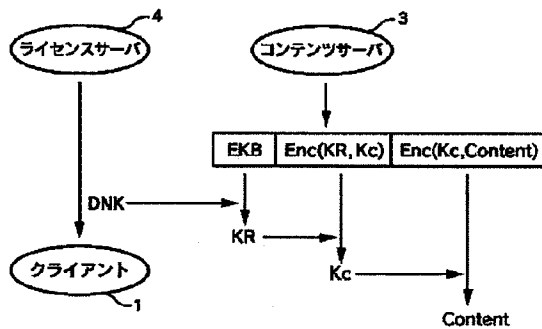
【図16】

図16

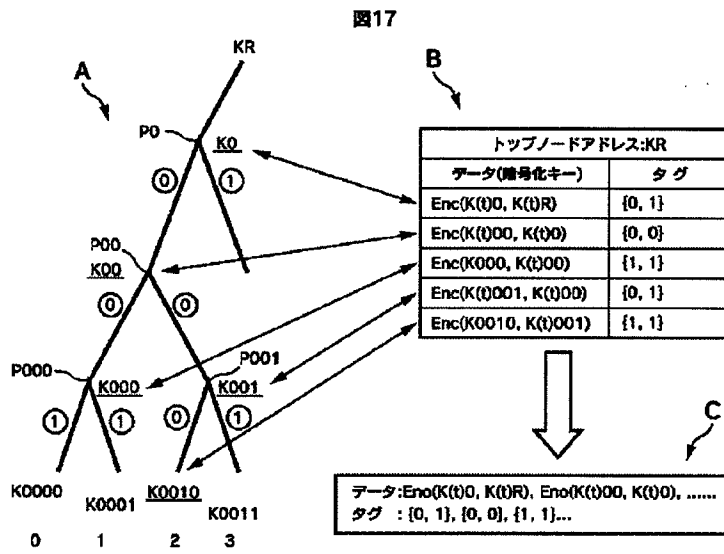


【図18】

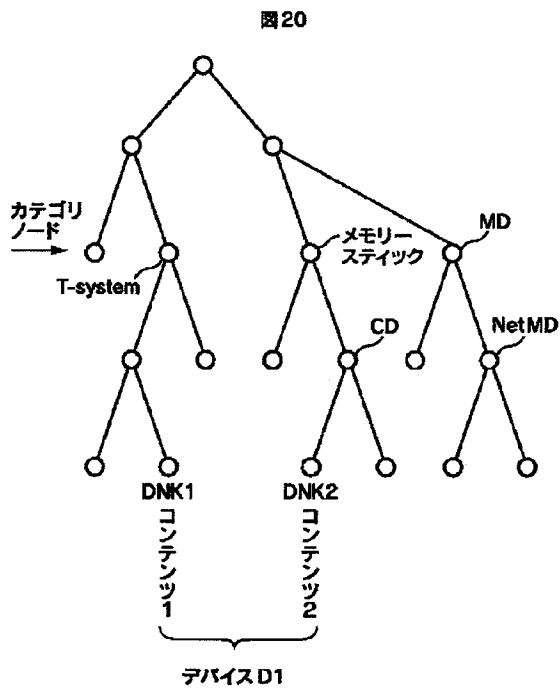
図18



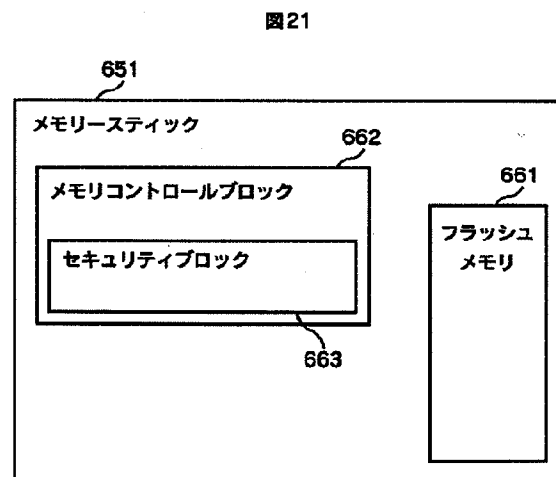
【図17】



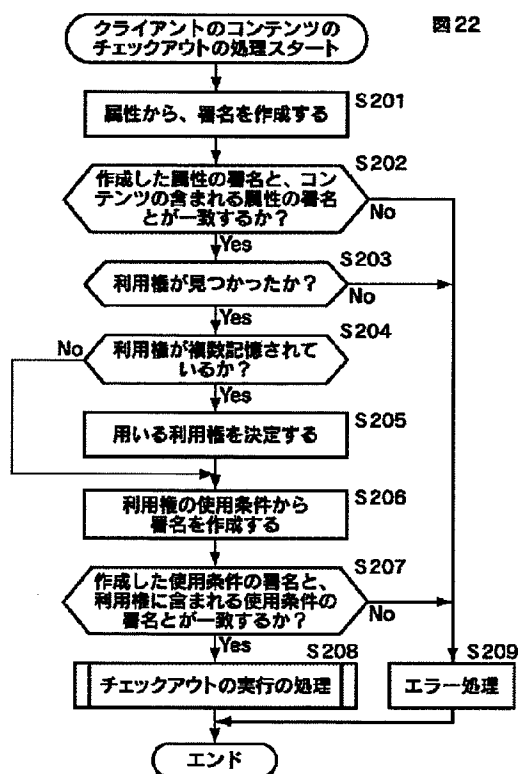
【図20】



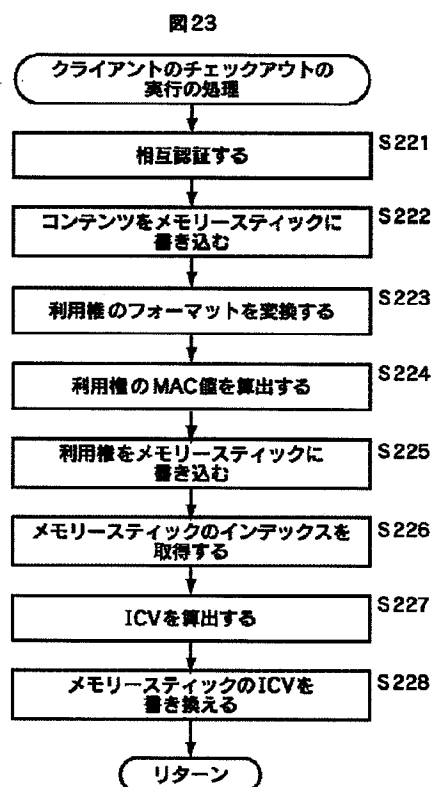
【図21】



【図22】

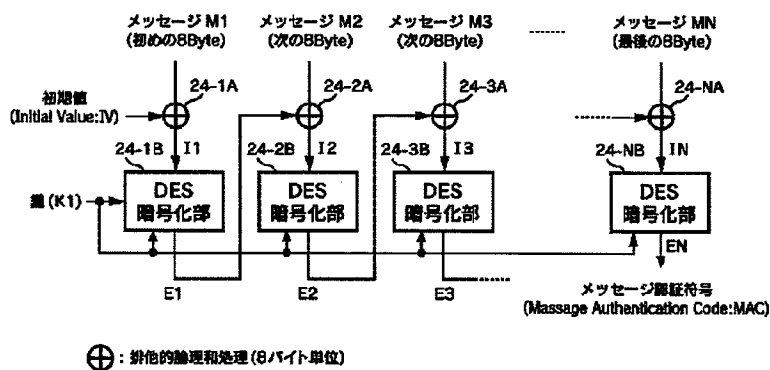


【図23】



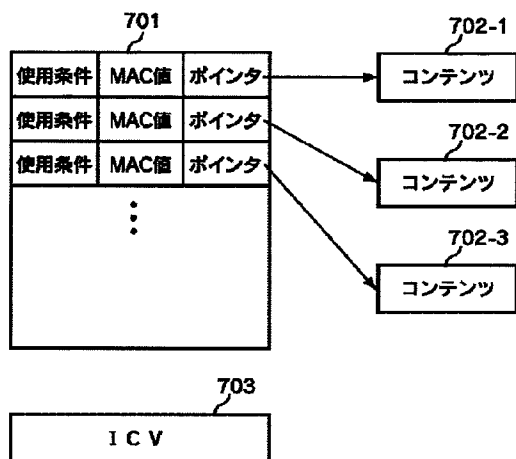
【図24】

図24



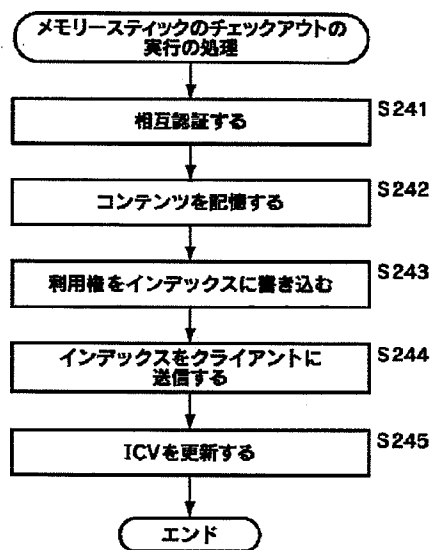
【図25】

図25



【図26】

図26



フロントページの続き

(72)発明者 二神 基誠
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5B017 AA07 BA05 BA09 CA15 CA16
5J104 AA09 AA12 AA15 PA14